Initailization Phase (one time)

Content Provider Client upon client access an applet (containing Kc) is downloaded 1. picks random a and sends: 11 IDu, IDm, g^a 2. picks random b and Nb, calculates Kab = $g^(a^*b)$ and sends: 12 PWu(g^b), Kab(Nb) 3. calculates Kab, picks random Na and sends: 13 Kab(Na), MAC(Kab, Na Nb) 4. Verifies MAC, stores Kab, stores IDm and sends: 14 MAC(Kab, Nb Na) 5. verifies MAC and stores PW*(Kc(Kab)) Kc is hidden key of Content Provider used by applet on the client machine *note this does not necessairly have to match PWu

Fig. 1

Access Phase

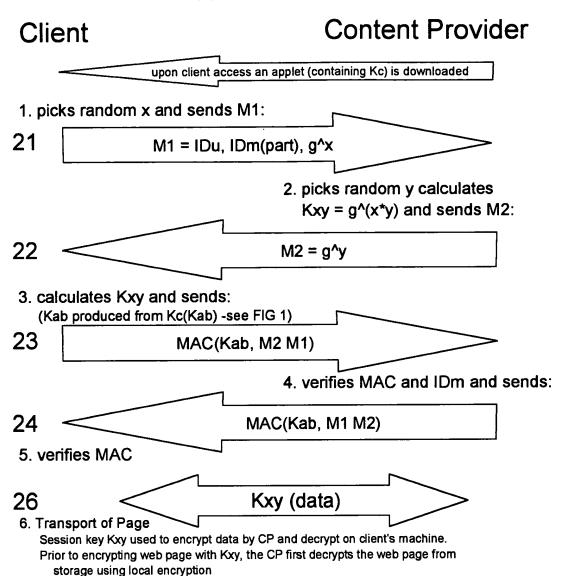


Fig. 2

3 YO999-558

Table of Information kept by Content Provider

Users	IDm	IDu	PWu	Kab
User1				
User2				
User3				
User4				

Fig. 3